

Hon. David R. Grand U. S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 23-mc-50751-2	Date and time warrant executed: 7/19/23	Copy of warrant and inventory left with: N/A
----------------------------	--	---

Inventory made in the presence of : N/A

Inventory of the property taken and name of any person(s) seized:
Data files from extraction of two cell phones**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 7/24/23



Executing officer's signature

Lorin Folk, HSI SA

Printed name and title

ATTACHMENT A

DESCRIPTION OF THE PROPERTY TO BE SEARCHED

Cellular telephone (referred to as the “TARGET TELEPHONES”) currently in law enforcement possession – namely in HSI evidence storage at the HSI’s offices, located at 11301 Metro Airport Center Drive, Romulus, Michigan – more thoroughly and individually described below:

f. iPhone X with black back / IMEI: 354868096239720/ S/N:

GHLHR00JJCLH (TARGET TELEPHONE 1)

g. iPhone 13 Pro with blue back/ IMEI 356314951575856/ S/N

CQDC24FJPL (TARGET TELEPHONE 2)

This warrant authorizes the forensic examination of the TARGET TELEPHONES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

A. All information, records, and content contained in the TARGET TELEPHONES, described in Attachment A, that relate to violations of U.S.C. § 1028 (identity theft), 18 U.S.C. 1028A (aggravated theft), 18 U.S.C. § 1341 (mail fraud), and 18 U.S.C. 1343 (wire fraud), involving KENNY HOWARD III since April 2020, including:

a. Contact list, which provides the names and/or nicknames and phone numbers, including cellular, home and work numbers of persons in contact with the users of the TARGET TELEPHONES that pertain to the above described criminal activity;

b. Text, e-mail, voicemail, social media (e.g., Facebook, Instagram, Twitter) messages that relate to the underlying offenses described in paragraph A;

c. Pictures and videos which includes any saved pictures or videos taken, sent or received and their metadata that relate to the underlying offenses described in paragraph A;

d. Notepad or other files that allows the user to input and store miscellaneous information into the phone that may relate to the underlying offenses described in paragraph A ;

e. Calendar, which allows the user to store dates and/or times of appointments and events that may relate to the underlying offenses described in paragraph A;

f. Call history, including all incoming and outgoing calls, call logs and related identifying information including the telephone number, date, and time of calls made to and from the TARGET TELEPHONES, received, dialed calls, including times and contact information, that may relate to the underlying offenses described in paragraph A;

g. Any information related to sources of PII used to commit the underlying offenses described in paragraph A (including names, addresses, phone numbers, or any other identifying information);

h. Any information recording users of the TARGET TELEPHONES' schedule or travel that may relate to the underlying offenses described in paragraph A;

i. All bank records, checks, credit card bills, account information, and other financial records that relate to the underlying offenses described in paragraph A;

j. Information related to financial, banking, or debit or credit card transactions that relate to the underlying offenses described in paragraph A;

k. Any information regarding the past location of the TARGET TELEPHONES that may show the locations of the fruits of the crimes described in

paragraph A, or the location of HOWARD or a co-conspirator while committing the offenses ;

l. Information related to any of the victims of the crimes identified above;

m. All information, records, and content contained in the TARGET TELEPHONES regarding wire fraud, aggravated identity theft, mail fraud and unemployment insurance fraud by HOWARD, or co-conspirators;

n. Evidence of user attribution showing who used or owned the cellular telephones at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

o. Records evidencing the use of the Internet Protocol addresses to communicate with various State Unemployment Insurance websites, including:

1. records of Internet Protocol addresses used;
2. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage

(such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI, and/or the DOL-OIG may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.